

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2001-331106  
(P2001-331106A)

(43) 公開日 平成13年11月30日 (2001. 11. 30)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テ-マ-ト* (参考)
G 0 9 C 5/00		G 0 9 C 5/00	
G 0 6 T 1/00	5 0 0	G 0 6 T 1/00	5 0 0 B
G 1 1 B 20/10		G 1 1 B 20/10	H
20/12		20/12	
H 0 4 L 9/08		H 0 4 N 1/387	

審査請求 未請求 請求項の数20 O L (全 22 頁) 最終頁に続く

(21) 出願番号 特願2001-59717(P2001-59717)  
(22) 出願日 平成13年3月5日 (2001. 3. 5)  
(31) 優先権主張番号 特願2000-70020(P2000-70020)  
(32) 優先日 平成12年3月14日 (2000. 3. 14)  
(33) 優先権主張国 日本 (J P)

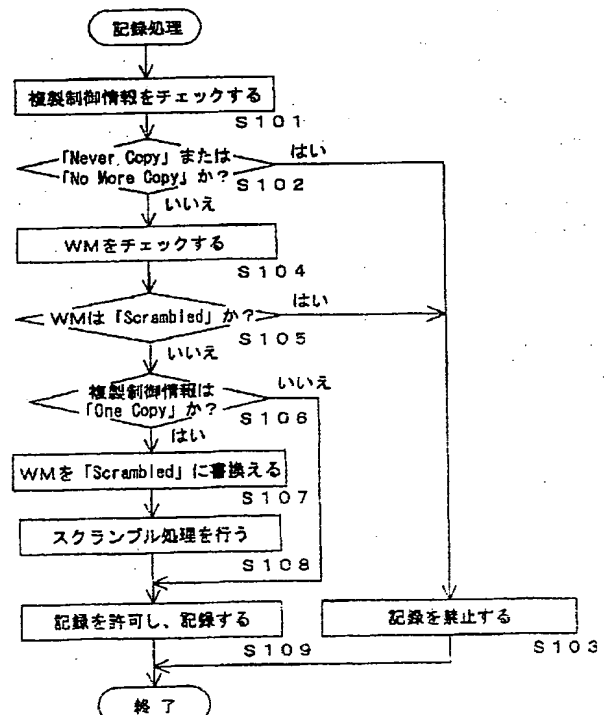
(71) 出願人 000005821  
松下電器産業株式会社  
大阪府門真市大字門真1006番地  
(72) 発明者 永井 隆弘  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内  
(72) 発明者 石原 秀志  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内  
(72) 発明者 福島 能久  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内  
(74) 代理人 100062144  
弁理士 青山 葆 (外2名)

(54) 【発明の名称】 暗号化情報信号、情報記録媒体、情報信号再生装置、および、情報信号記録装置

(57) 【要約】

【課題】 記録媒体の種類にかかわらず、不正に作成された記録媒体からの情報信号の再生を実質的に不能にでき、有効かつ安価に複製の防止ができるようにする。

【解決手段】 複製制御の対象とされる情報信号を暗号化した暗号化情報信号であって、前記情報信号は、前記情報信号が暗号化された状態の信号であることを識別する識別情報が電子透かし情報として重畳された信号である、暗号化情報信号、その信号を記録した情報記録媒体、その信号を再生する情報信号再生装置、および、その信号を記録する情報信号記録装置を提供する。



BEST AVAILABLE COPY

# 【特許請求の範囲】

【請求項1】 複製制御の対象とされる情報信号を暗号化した暗号化情報信号であって、前記情報信号は、前記情報信号が暗号化された状態の信号であることを識別する識別情報が電子透かし情報として重畳された信号である、暗号化情報信号。

【請求項2】 前記情報信号は、これ以上の複製禁止、および、絶対複製禁止の少なくとも一方の制限が課された情報信号である、請求項1に記載の暗号化情報信号。

【請求項3】 前記電子透かし情報は、前記暗号化情報信号が記録される情報記録媒体の種別を表す種別情報をさらに含む、請求項1に記載の暗号化情報信号。

【請求項4】 請求項1に記載の暗号化情報信号が記録された情報記録媒体。

【請求項5】 暗号化された第1の鍵と、暗号化された第2の鍵とがさらに記録された情報記録媒体であって、前記第1の鍵は、電子透かし情報が重畳された前記情報信号を暗号化するために用いられた鍵であり、前記第2の鍵は、前記第1の鍵を暗号化するために用いられた鍵である、請求項4に記載の情報記録媒体。

【請求項6】 請求項4に記載の情報記録媒体から暗号化情報信号を読み出す読み出し部と、

読み出し部が読み出した前記暗号化情報信号が暗号化されている状態であることを判別する暗号化状態判別部と、

前記暗号化情報信号を解読して電子透かし情報が重畳された情報信号を取り出す解読部と、

解読部が解読した前記情報信号から前記電子透かし情報を抽出して、前記識別情報の示す内容を判別する電子透かし情報デコード部と、

暗号化状態判別部により判別された状態と、電子透かし情報デコード部により判別された識別情報の示す状態とを比較し、一致しない場合には前記情報信号の再生を禁止する再生制御部と、

を備えた情報信号再生装置。

【請求項7】 暗号化状態判別部は、解読部が情報信号を取り出した場合には、前記暗号化情報信号は暗号化されている状態であると判別する、請求項6に記載の情報信号再生装置。

【請求項8】 前記電子透かし情報は、前記暗号化情報信号が記録される情報記録媒体の種別を表す種別情報をさらに含む、

情報信号再生装置は、前記情報記録媒体の種別を判別する種別判別部をさらに備え、

前記種別情報により表された情報記録媒体の種別と、種別判別部により判別された情報記録媒体の種別とが一致する場合に、再生制御部は前記情報信号の再生を許可する、請求項6に記載の情報信号再生装置。

【請求項9】 前記情報記録媒体には、暗号化された第1の鍵と、暗号化された第2の鍵とがさらに記録されて

おり、前記第1の鍵は、電子透かし情報が重畳された前記情報信号を暗号化するために用いられた鍵であり、前記第2の鍵は、前記第1の鍵を暗号化するために用いられた鍵であり、

解読部は、前記第2の鍵を暗号化するために用いられ、情報信号再生装置に固有に割り当てられた第3の鍵を保持しており、前記第3の鍵で暗号化された第2の鍵を解読して前記第2の鍵を取得し、取得した前記第2の鍵で暗号化された第1の鍵を解読して前記第1の鍵を取得し、取得した前記第1の鍵で前記暗号化情報信号を解読して電子透かし情報が重畳された情報信号を取り出す、請求項6に記載の情報信号再生装置。

【請求項10】 情報信号再生装置は、読み出し部、暗号化状態判別部、および、種別判別部を含み、さらに第1の認証部を含むドライブ装置と、解読部、電子透かし情報デコード部、および、再生制御部を含み、さらに第2の認証部を含むデコード装置と、ドライブ装置とデコード装置とを接続するインターフェースとから構成されており、

前記第1の認証部と前記第2の認証部とは、前記インターフェースを介して通信して、前記第1の認証部はデコード装置がコンプライアントな装置であるか否かを認証し、前記第2の認証部はドライブ装置がコンプライアントな装置であるか否かを認証し、

前記第1の認証部と前記第2の認証部との間で認証が成立した場合に、再生制御部は前記情報信号の再生を許可する、請求項8に記載の情報信号再生装置。

【請求項11】 前記情報記録媒体には、前記第1の認証部および前記第2の認証部がそれぞれ認証に用いる、第1の認証鍵および第2の認証鍵がさらに記録されており、

第1の認証部は、ドライブ装置に固有に割り当てられた第1のデバイス鍵を有し、前記第1の認証鍵と、前記第1のデバイス鍵と、種別判別部が判別した前記情報記録媒体の種別とに基づいて第1の媒体認証鍵を生成し、第2の認証部は、デコード装置に固有に割り当てられた第2のデバイス鍵を有し、前記第2の認証鍵と、前記第2のデバイス鍵とに基づいて、第2の媒体認証鍵を生成し、

前記第1の認証部と前記第2の認証部とは、第1の媒体認証鍵と第2の媒体認証鍵とを比較して認証を行う、請求項10に記載の情報信号再生装置。

【請求項12】 第2の認証部は、情報記録媒体ごとに異なる認証手順、および、情報信号転送手順のうちの少なくとも一方を利用して情報記録媒体種別を検出する、請求項11に記載の情報信号再生装置。

【請求項13】 複製制御の対象とされる情報信号を情報記録媒体に記録する情報信号記録装置であって、前記情報信号が暗号化された状態の信号であることを識別する識別情報を、電子透かし情報として情報信号に重

置する電子透かし情報処理部と、  
電子透かし情報処理部により前記電子透かし情報が重畳された情報信号を暗号化して暗号化情報信号を生成する暗号化部と、  
暗号化部により生成された暗号化情報信号を、情報記録媒体に書き込む書き込み部とを備えた情報信号記録装置。

【請求項14】 前記情報記録媒体の種別を判別する種別判別部をさらに備え、  
前記電子透かし情報は、種別判別部により判別された、前記暗号化情報信号が記録される情報記録媒体の種別を表す種別情報をさらに含む、請求項13に記載の情報信号記録装置。

【請求項15】 情報信号に重畳されている電子透かし情報を抽出して、前記識別情報の示す内容を判別する電子透かし情報デコード部と、  
電子透かし情報デコード部により判別された前記識別情報に基づいて、記録を許可する記録制御部とをさらに備えた請求項14に記載の情報信号記録装置。

【請求項16】 情報信号記録装置は、  
書き込み部、種別判別部を含み、さらに第1の認証部を含むドライブ装置と、  
暗号化部、電子透かし情報処理部、電子透かし情報デコード部、および、記録制御部を含み、さらに第2の認証部を含むエンコード装置と、  
ドライブ装置とエンコード装置とを接続するインターフェースとから構成されており、  
前記第1の認証部と前記第2の認証部とは、前記インターフェースを介して通信して、前記第1の認証部はエンコード装置がコンプライアントな装置であるか否かを認証し、前記第2の認証部はドライブ装置がコンプライアントな装置であるか否かを認証し、  
前記第1の認証部と前記第2の認証部との間で認証が成立した場合に、記録制御部は前記情報信号の記録を許可する、請求項15に記載の情報信号記録装置。

【請求項17】 前記情報記録媒体には、前記第1の認証部および前記第2の認証部がそれぞれ認証に用いる、第1の認証鍵および第2の認証鍵がさらに記録されており、  
第1の認証部は、ドライブ装置に固有に割り当てられた第1のデバイス鍵を有し、前記第1の認証鍵と、前記第1のデバイス鍵と、種別判別部が判別した前記情報記録媒体の種別とに基づいて第1の媒体認証鍵を生成し、  
第2の認証部は、エンコード装置に固有に割り当てられた第2のデバイス鍵を有し、前記第2の認証鍵と、前記第2のデバイス鍵とに基づいて、第2の媒体認証鍵を生成し、  
前記第1の認証部と前記第2の認証部とは、第1の媒体認証鍵と第2の媒体認証鍵とを比較して認証を行う、請求項16に記載の情報信号記録装置。

【請求項18】 第2の認証部は、情報記録媒体ごとに異なる認証手順、および、情報信号転送手順のうちの少なくとも一方を利用して情報記録媒体種別を検出する、請求項17に記載の情報信号記録装置。

【請求項19】 前記情報記録媒体には、情報信号再生装置に固有に割り当てられた第3の鍵で暗号化された第2の鍵が記録されており、  
暗号化部は、  
暗号化部の内部で発生させた乱数、前記情報記録媒体に記録された第1の鍵情報、および、電波に重畳された第1の鍵情報のいずれかに基づいて前記第1の鍵を取得して、前記電子透かし情報が重畳された情報信号を第1の鍵で暗号化し、  
前記第1の鍵を第2の鍵で暗号化し、  
第3の鍵と、情報記録媒体に記録された暗号化された第2の鍵とに基づいて第2の鍵を取得する、請求項13に記載の情報信号再生装置。

【請求項20】 書き込み部は、第2の鍵で暗号化された第1の鍵をさらに情報記録媒体に書き込む、請求項19に記載の情報信号記録装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタル化された著作物、例えば映像、音楽等の情報信号を情報記録媒体に記録する際の不正な複製を制限する技術、および、不正に複製された情報記録媒体からの再生を制限する技術に関する。

【0002】

【従来の技術】近年、デジタルコンテンツの普及に伴い、デジタルコンテンツの不正な複製による著作権侵害が大きな問題となっている。不正な複製を防止するために、デジタルコンテンツに複製制御のための情報（複製制御情報）を付加したり、または、暗号化技術を用いて情報信号を暗号化し、正式にライセンスを受けた機器以外の機器には復号化（解読）できないようにする技術が考えられている。また、情報信号に対して、複製制御情報をさらに電子透かし情報としても埋め込む技術も存在する。電子透かし情報は雑音として情報信号に重畳され、容易に書き換えられないので、複製制御情報が不正に書き換えられた場合でも再生制御および記録制御を行うことができる。

【0003】複製制御のために情報信号に付加される情報は、“複製可能（Copy Free）”、“1回複製可能（One Copy）”、“これ以上複製禁止（No More Copy）”、“絶対複製禁止（Never Copy）”の4状態がある。この4状態によって、情報信号の複製世代や複製制限状態を表現できる。

【0004】複製の制限は、以下のようにして行われる。すなわち記録装置が画像、音声等の情報信号に含ま

れる複製制御情報をチェックし、複製制御情報が“これ以上複製禁止”や“絶対複製禁止”を表す場合は記録を制限する。これにより、複製世代制限が実現される。しかしながら、複製制御情報をチェックしない記録装置は“これ以上複製禁止”の状態にある情報信号でも記録媒体に記録することができ、さらにこの記録媒体は、複製制御情報を含む元の情報信号と同じ情報信号がそのまま複製された記録媒体である。これでは著作権が保護できない。

【0005】この問題を解決するための技術として、特開平11-353796号公報には、情報信号にさらに電子透かし情報を重畳し、情報信号の再生時に電子透かし情報が示す状態を書き換えることにより、不正に記録された記録媒体からの再生を実質的に不能とする技術が記載されている。

【0006】より具体的に説明する。この説明中、電子透かし情報の解読処理または書き込み処理に対応することを「コンプライアント」、対応しないことを「ノンコンプライアント」という。図16は、従来の複製制御の原理を示す図である。DVD-RAM等のRAMディスク1300には、“これ以上の複製禁止”を示す複製制御情報(CGMS[11])と、同様に“これ以上の複製禁止”を示す電子透かし情報(WM [No More Copy])とが重畳された情報信号が記録されている。この情報信号の再生に際し、コンプライアント再生装置1301は、電子透かし情報を“No More Copy”(これ以上の複製禁止)から、“Never Copy”(絶対複製禁止)に書き換え、情報信号に重畳し直した上で情報信号を再生出力信号として送出する。DVD-RAMでは通常、複製を禁止する場合には“No More Copy”が利用され、“Never Copy”は利用されない。したがって、情報信号に重畳されている電子透かし情報が“Never Copy”であることを検出すると、コンプライアント記録装置1302はその情報信号を記録しない。これにより複製を制御できる。

【0007】一方、ノンコンプライアント記録装置1303は、電子透かし情報の内容にかかわらず記録制限なく情報信号を別のRAMディスク1304へ記録する。しかしながら、不正に記録されたRAMディスク1304の電子透かし情報は“Never Copy”である。したがって、コンプライアント再生装置1305は、その電子透かし情報を読み取ることでそのRAMディスク1304を不正な複製が行われた記録媒体であると判定し、再生を実質的に不能とする。

【0008】

【発明が解決しようとする課題】上述のように従来のコンプライアント再生装置1301は、複製を制御するために、電子透かし情報の内容を“No More Copy”(これ以上の複製禁止)から、“Never Copy”(絶対複製禁止)に書き換える。このため、再生装置は電子透かし情

報の書き換え手段を備えることが不可欠であり、再生装置のコストアップにつながる。

【0009】また上述の技術は、DVD-ROMには適用できない。DVD-ROMでは、不正か否かを判定するための電子透かし情報“Never Copy”が、通常の使用においてディスクに書き込まれるからである。

【0010】以上の点に鑑み、本発明の目的は、記録媒体の種類にかかわらず、不正に作成された記録媒体からの情報信号の再生を実質的に不能にすることにより、有効かつ安価に複製の防止ができるようにすることである。

【0011】

【課題を解決するための手段】上記課題を解決するために、本発明による複製世代管理は、複製制御が必要な情報信号を記録する情報記録媒体において、少なくとも、これ以上の複製禁止、絶対複製禁止の状態の情報信号である前記情報信号には情報記録媒体にスクランブル状態で記録されることを示すスクランブル情報が電子透かし情報として重畳され、前記電子透かし情報が重畳された情報信号にスクランブルを施した情報信号であることを特徴とする。

【0012】本発明の情報記録再生装置は、これ以上の複製禁止、あるいは、絶対複製禁止の状態である前記情報信号には、情報記録媒体にスクランブル状態で記録されることを示すスクランブル情報が電子透かし情報として重畳され、前記電子透かし情報が重畳された情報信号にスクランブルを施した情報信号として記録された情報記録媒体を読み出す情報再生装置であって、情報記録媒体から情報を読み出す情報読み出し手段と、前記情報信号に対して施されたスクランブルをデスクランブルするデスクランブル手段と、デスクランブルされた情報信号に電子透かし情報として重畳されているスクランブル情報を検出する電子透かし情報検出手段と、前記電子透かし情報とデスクランブル手段のデスクランブル動作を調べ、少なくとも、電子透かし情報のスクランブル情報がスクランブル状態にあり、デスクランブル手段が動作していない場合に、前記情報信号の正常な再生を禁止する再生制御手段とを備える。

【0013】本発明の情報記録装置は、1回複製可能、これ以上の複製禁止、あるいは、絶対複製禁止の状態の複製制御情報を有する前記情報信号を情報記録媒体に書き込む情報記録装置であって、前記複製制御情報を検出する手段と、検出した複製制御情報が1回複製可能である場合に、情報記録媒体にスクランブル状態で記録されることを示すスクランブル情報が電子透かし情報として前記情報信号に重畳する電子透かし情報書換手段と、前記電子透かし情報を重畳した情報信号にスクランブルを施すスクランブル手段と、前記スクランブルした情報信号を情報記録媒体に書き込む情報書き込み手段を備える。

【0014】本発明の情報信号記録装置は、1回複製可能、これ以上の複製禁止、あるいは、絶対複製禁止の状態の複製制御情報を有する前記情報信号を情報記録媒体に書き込む情報記録装置において、前記複製制御情報を検出する複製制御情報検出手段と、前記情報信号に重畳されている電子透かし情報を検出する電子透かし情報検出手段と、前記電子透かし情報として情報信号がスクランブル状態で記録されていることを示すスクランブル情報が検出された場合に、記録を禁止する記録制御手段とを備える。

【0015】

【発明の実施の形態】以下、添付の図面を参照して、本発明による暗号化情報信号、情報記録媒体、情報信号再生装置、および、情報信号記録装置を説明する。実施の形態では、情報記録媒体はDVD-RAM (ROM) に代表される光ディスクであり、この光ディスクに情報信号が記録される。また複製制御の対象は、画像、音声等を表す情報信号、すなわち画像音声情報である。

【0016】以下の説明では、記録型のDVDをRAMディスク、再生専用のDVDをROMディスクと称する。また、後述の複製世代制限処理に対応する記録装置および再生装置をコンプライアントの装置と呼び、複製世代制限処理に対応していない装置をノンコンプライアントの装置と呼ぶ。

【0017】(実施の形態1) 図1は、本実施の形態による複製世代管理方法を説明するための概略図である。本実施の形態では、ROMディスク100には映像や音声などの情報信号が記録されている。ただし、ROMディスクに代えてRAMディスクを利用してよい。

【0018】まず、本実施の形態における情報信号を説明する。情報信号には、映像や音声などを表す信号の他に、雑音の形で電子透かし情報WM (digital WaterMark) が埋め込まれている。電子透かし情報の特徴は、主に、著作物 (映像や音声) の改変や圧縮、伸張処理を行っても電子透かし情報が消えないこと、人間の目や耳では感知しにくいレベルで電子透かし情報が埋め込まれること、および、電子透かし情報を埋め込んでもオリジナルの著作物の品質が保持されることである。この特徴により、不正な書き換えを防止し、再生制御および記録制御を行うことができる。

【0019】情報信号にはさらに、複製制御情報 (図示せず) も記録されている。複製制御情報は、コピー可能か否かを表現できる情報である。例えば、2ビットの情報を用いるCGMS (Copy Generation Management System) である。CGMSによれば、“00”は「複製フリー」、「01」は「1回複製可能」、「10」は「絶対複製禁止」、そして“11”は「これ以上の複製禁止」を表す。

【0020】情報信号を複製制御の対象とする場合、例えば情報信号の複製を全く禁止する場合には、正規にラ

イセンスを受けた装置でなければ情報信号を再生できないようにするために、本発明では情報信号をスクランブル (暗号化) して記録する。本発明の特徴的な処理は、情報信号がスクランブルされた情報であることを示すスクランブル情報 “Scrambled” を、電子透かし情報WMとして情報信号に重畳することである。したがってスクランブル情報は、情報信号が暗号化されているか否かの状態を識別するために用いられる暗号状態の識別情報ということができる。電子透かし情報を用いた複製制御の詳細な説明は後述する。上述の電子透かし情報の特徴によれば、スクランブル情報 “Scrambled” は信号情報の改変、圧縮または伸張処理にかかわらず消えることはないので、検出することができる。スクランブル処理は、電子透かし情報が重畳された情報信号に対して、特定のスクランブル方式 (暗号方式) にしたがって行われる。

【0021】一方、情報信号を複製制御の対象としない場合、例えば、情報信号の自由な複製を許す場合には、情報信号はスクランブルされない。この場合には、信号情報には電子透かし情報が重畳されても、されなくてもよい。電子透かし情報が重畳される場合には、電子透かし情報は、信号情報がスクランブルされていないことを示すスクランブル情報 “Non-Scrambled” となる。記録装置 (図示せず) は、スクランブルされていない情報信号をそのまま、または電子透かし情報を重畳した情報信号をディスクに記録し、ROMディスク100を製造する。

【0022】本発明の複製世代管理方法を説明するに先だて、まずROMディスク100を製造する際のスクランブル処理の手順を説明する。以下説明するスクランブル処理は、ROMディスク100の製造業者がオーサリングシステムおよびディスクカッティングシステムを利用して行う。スクランブル処理の例は、DVD-ROMの著作権保護システムCSS (Content Scramble System) である。映像、音声等を含む情報信号は、3種類の暗号鍵を階層的に用いて暗号化される。3種類の暗号鍵とは、タイトル鍵、ディスク鍵、および、マスター鍵である。以下、著作権保護システムCSSのコンテンツ暗号化手順に沿って説明する。本明細書では、「スクランブル」という語は「暗号化」を意味する。スクランブルのための暗号方式は、1つの鍵を用いて暗号化を行うアルゴリズムであればよい。したがって、周知のアルゴリズムが利用可能である。アルゴリズムの説明は省略する。なお、このアルゴリズムはセキュリティの観点から非公開とされることが多い。一方、スクランブルされた情報をスクランブルされていない情報に戻すことを「デスクランブル」という。これは、「解読」または「復号化」という語と同義である。

【0023】スクランブル処理の手順は以下のとおりである。まず、情報信号がMPEG圧縮され、その後、タ

タイトル鍵を用いてスクランブルされる。タイトル鍵は、著作権者、例えば映画のディレクタがディスクに格納されるタイトル毎、すなわち情報信号の単位毎に自由に選んだ鍵である。スクランブルされた信号情報は、ディスクのデータ記録領域に格納される。

【0024】次に、タイトル鍵は、ディスク鍵を用いて暗号化される。ディスク鍵とは、著作権管理者、例えば映画会社がディスク毎に自由に選ぶことができる鍵である。ディスクが1つ以上の暗号化タイトルを含む場合、著作権管理者は自由にディスク鍵を決定できる。暗号化されたタイトル鍵は、ユーザがアクセスできない、ディスクのセクターヘッダ領域に格納される。

【0025】最後に、ディスク鍵はマスター鍵を用いて暗号化され、暗号化されたディスク鍵セットに変換される。マスター鍵とは、スクランブルされた情報信号を復号化するデスクランブル装置のメーカー毎に割り当てられた鍵であり、メーカー毎に異なる。「暗号化されたディスク鍵セット」とは、暗号化されたディスク鍵が1または複数存在することを意味する。これはライセンスを受けたメーカーの数だけマスター鍵が存在するので、その数と同じ数の1以上のディスク鍵が生成されるからである。暗号化されたディスク鍵セットは、ユーザがアクセスできない、ディスクのリードイン領域に格納される。

【0026】以上の処理により、ROMディスク100には、スクランブルされた信号情報、暗号化されたタイトル鍵、および、暗号化されたディスク鍵セットが格納されていることになる。

【0027】複製制御の対象となるROMディスク100の情報信号を再生するためには、デスクランブル処理を行う必要がある。デスクランブル処理を行うためには、上述の所定の暗号方式に対するライセンスを受け、復号鍵（マスター鍵）や復号アルゴリズムに関する情報を取得しなければならない。図1に示すような、復号機能を実装したコンプライアント再生装置101では、ROMディスク100からスクランブルが施されている情報信号を読み出し、デスクランブルを行い、MPEGデコード可能な情報信号を得ることができる。

【0028】以下では、DVDプレーヤ等の再生機器が行うデスクランブル処理を説明し、次にDVD-RAMドライブ等の記録装置が行うスクランブル処理を説明する。図2は、スクランブルされた信号情報の読み出しまたは書き込みを行う際のデータの流れを示す図である。

【0029】図2の(a)は、ディスク210に記録された、スクランブルされた情報信号をデスクランブル処理する概念図を示す。ディスク210は、ROMディスク100（図1）に相当するディスクであり、スクランブルされた情報信号212と、暗号化されたタイトル鍵214と、暗号化されたディスク鍵セット216とが記録されている。ここでは、スクランブルされた情報信号212はMPEG圧縮された映像音声情報とする。再生

機器のデスクランブル部220は、情報信号をデスクランブルし、MPEGデコードする装置である。デスクランブル部220は、ディスク鍵復号化部222と、タイトル鍵復号化部224と、情報信号復号化部226と、MPEGデコーダ228とを含む。

【0030】デスクランブル部220は、暗号化されたディスク鍵セット216、暗号化されたタイトル鍵、および、スクランブルされた情報信号をディスク210から読み出す。ディスク鍵復号化部222はまず、内部記憶領域（図示せず）に保持した、または再生機器の他の構成要素を介して与えられたマスター鍵を用いて、読み出したディスク鍵セット216から自己のディスク鍵を復号化する。次にタイトル鍵復号化部224は、復号化したディスク鍵を用いて暗号化されたタイトル鍵214を復号化する。そして情報信号復号化部226は、復号化したタイトル鍵を用いてスクランブルされた情報信号212を復号化する。このようにしてデスクランブル処理が行われる。デスクランブルされた情報信号はMPEG圧縮処理されたデータであるので、本実施の形態ではMPEGデコーダ228がデコード処理を行って、映像音声情報を出力する。以上、デスクランブル部220の処理を説明した。

【0031】図2の(b)は、ディスク230に記録するために、情報信号をスクランブル処理する概念図を示す。この処理は、例えば「1回複製可能」とされた情報信号を記録する際の処理である。書き込みに用いられるディスク230は、製造業者からの出荷時に予め暗号化されたディスク鍵セット236が記録されている。

【0032】まずスクランブル部240のMPEGエンコーダ248は、入力された情報信号をMPEG圧縮処理し、生成したMPEGデータを情報信号暗号化部246に送る。次に、情報信号暗号化部246は、タイトル鍵を用いてMPEGデータをスクランブル処理する。タイトル鍵は乱数発生器250で生成された乱数である。一方タイトル鍵暗号化部244は、ディスク鍵を用いてタイトル鍵を暗号化する。暗号化されたタイトル鍵234はディスク230に記録される。ここで、ディスク鍵は、スクランブル部240が保持するマスター鍵を用いて、ディスク230に記録された暗号化されたディスク鍵セット236から、その記録装置のメーカーに対応するディスク鍵を復号化することにより得られる。

【0033】なお一度タイトル鍵を生成し、暗号化されたタイトル鍵234としてディスク230に記録すると、その後に情報信号をスクランブル処理して記録する際には記録された暗号化されたタイトル鍵234が用いられる。すなわち、スクランブル部240はディスクの暗号化されたタイトル鍵234を読み出してディスク鍵で復号化し、タイトル鍵を用いて情報信号をスクランブルする。

【0034】以上のように、スクランブル部240は、

2通りの経路でタイトル鍵を取得することができる。すなわち、乱数発生器250で発生された乱数をタイトル鍵として取得する場合と、ディスク230に記録された暗号化されたタイトル鍵234を復号化してタイトル鍵として取得する場合の2つの場合である。将来、番組配信が増加すると、放送業者（コンテンツ製作者）の側でタイトル鍵を生成し、そのタイトル鍵でスクランブルされた情報信号が、デジタル放送として、電波で配信されると考えられる。この場合には、ディスクには、放送業者から取得したタイトル鍵とスクランブルされた情報信号を記録することになる。

【0035】以上のようにして、情報信号のスクランブル処理およびデスクランブル処理を行う。

【0036】次に再び図1を参照して、本発明による複製世代管理の原理を説明する。本実施の形態では、信号情報を複製制御の対象とする場合には、その信号情報にはスクランブル情報“Scrambled”が電子透かし情報として重畳されている。ROMディスク100には、スクランブル情報“Scrambled”が重畳された信号情報がスクランブルされて記録されているとする。

【0037】本発明による複製世代管理の主たる特徴は、ディスク上の信号情報のスクランブル状態（すなわちスクランブルされているか否か）と、スクランブル情報の状態（すなわちスクランブル情報が“Scrambled”となっているか否か）とを比較し、比較結果に応じて再生または記録を行うか、それらを制限するかを決定することである。信号情報がスクランブルされているか否かは、信号情報や、関連する付属ファイルの情報の中に所定のフラグが立っているか否か、またはデスクランブル部が正常に動作したか否かで判断する。以下、具体的に説明すると、まず再生装置101は、まずROMディスク100からスクランブルされた信号情報を読み出して、デスクランブルを行う。そして再生装置101はデスクランブルされた信号情報からスクランブル情報を検出し、スクランブル状態が一致するか否かの比較を行う。ここでは、信号情報がスクランブルされている状態であったこと、および、スクランブル情報が“Scrambled”であることから、スクランブル状態は一致すると判断できる。これによりコンプライアント再生装置101はデスクランブルした情報信号の出力を行う。このとき留意すべきは、出力される情報信号にはスクランブル情報“Scrambled”が重畳されていることである。電子透かし情報としてのスクランブル情報は、コンプライアント再生装置101のデスクランブル処理によっては消えることはないからである。

【0038】続いて、再生装置から出力された情報信号を記録媒体に不正に記録しようとした場合の、記録が制限される原理を説明する。コンプライアント記録装置102は、コンプライアント再生装置101からデスクラ

ンブルされた情報信号を受け取る。コンプライアント記録装置102は、受け取った信号情報がデスクランブル状態であること、および、重畳されたスクランブル情報が“Scrambled”であることを認識する。その結果、出力情報信号の状態とスクランブル情報の示す状態とが不一致なので、コンプライアント記録装置102はRAMディスク等の記録媒体への記録を行わない。これによりコンプライアント記録装置102では、信号情報の記録を制限できる。

【0039】一方、情報信号にスクランブルが施されていない場合も、同様に、スクランブル状態を比較すればよい。電子透かし情報が検出されない場合、あるいは電子透かし情報“Non-Scrambled”が検出された場合には情報信号の出力を行う。このように出力された信号は、自由に複製が可能であり、コンプライアント記録装置102ではRAMディスクへの情報信号の複製が許可される。

【0040】次に、情報信号がRAMディスクに不正に複製された場合に、再生が制限される原理を説明する。ノンコンプライアント記録装置103は、コンプライアント再生装置101が出力したデスクランブルされた情報信号を受け取る。この情報信号はスクランブル情報“Scrambled”を有するので複製制御対象であるが、ノンコンプライアント記録装置103は電子透かし情報を検出することなく、情報信号をRAMディスク104へ複製する。その後、コンプライアント再生装置105でこのようなRAMディスク104を再生しようとするとき、コンプライアント再生装置105は、スクランブル状態の比較を行う。この場合には、情報信号はデスクランブルされた状態で記録されている一方、情報信号にはスクランブルされていることを示すスクランブル情報“Scrambled”が重畳されている。よってコンプライアント再生装置105は、比較結果が不一致となることからそのRAMディスク104の情報信号は不正に複製された情報信号であると判断する。これによりコンプライアント再生装置105は、情報信号の再生を禁止する。

【0041】なお再生の制限は、記録の対象がRAMディスク104でない場合でも行われる。例えば、記録の対象が、書き込み可能であるが一旦書き込んだ後は読み出し専用のディスクとなるDVD-Rでもよい。

【0042】より確実に不正な記録および再生を禁止するために、スクランブルの際に用いられる暗号化アルゴリズムを記録媒体の種別に応じて相違させる手法もあわせて用いられている。例えば、DVD-ROM用の暗号化アルゴリズムとDVD-RAM用の暗号化アルゴリズムとを異ならせることにより、DVD-ROM用のアルゴリズムでスクランブルした情報信号をDVD-ROMからDVD-RAMに不正に複製したとしても、DVD-RAMからの再生を禁止できる、この動作を実現する

ためには、例えば、記録媒体の種別と、各種別に用いられる暗号化アルゴリズムとを対応付けるテーブルを設ける等すればよい。デスクランブル回路が、記録媒体の種別に対応する復号化アルゴリズムでデスクランブルできなかった場合には、不正に複製された記録媒体からの信号情報の再生を禁止できる。記録媒体の種別を表す種別情報は、スクランブル情報とともに電子透かし情報として情報信号に重畳されてもよい。種別情報は、記録される記録媒体の種別を表すことになる。したがって、DV D-Rに記録する場合と、DVD-RAMに記録する場合とも区別できる。

【0043】以上のように、本発明では、スクランブル（暗号化）された情報信号には、その情報信号が暗号化されていることを示す暗号化情報（スクランブル情報“Scrambled”）を電子透かし情報として重畳させる。信号情報は復号化された場合でも、電子透かし情報は改変されることなくそのままの内容で残る。信号情報が復号化状態（非暗号化状態）を示し、電子透かし情報は暗号化状態を示すので、その不一致を検出することにより、コンプライアント記録装置および再生装置のいずれにおいても、他の記録媒体への不正な記録または不正な記録媒体からの再生を禁止できる。よって、コンプライアント再生装置に電子透かし情報の書換手段を実装しなくても、ノンコンプライアント記録装置103によって行われた不正な複製ディスクをコンプライアント再生装置で再生禁止にできる。

【0044】なお、本実施の形態では、電子透かし情報として情報信号に施されているスクランブル情報（“Scrambled”、“Non-Scrambled”）を情報信号に重畳したが、情報信号のスクランブルの状態を示すものであれば他の情報を用いてよい。例えば、ROMディスクにおいて、複製制御情報である“絶対複製禁止”である情報信号に対して情報信号をスクランブルして記録する場合、この複製制御情報を電子透かし情報として情報信号に重畳しても同様の効果が得ることができる。

【0045】〔記録装置〕次に図3を参照して、コンプライアント記録装置102の構成を説明する。図3は、コンプライアント記録装置102の構成を示す。コンプライアント記録装置102は、デジタル入力端子301とアナログ入力端子302とを備える。各々は、暗号鍵情報等のデジタル信号と、映像音声情報等のアナログ信号とを接続された機器から受信する。暗号解読部303は、デジタル入力端子に接続される機器から送られてくる暗号鍵情報に基づいて暗号化されたデータを復号化し、圧縮ビデオデータを復元する。この際、入力された情報信号がコピー可能であるかどうかを示す複製制御情報を検出する。複製制御情報も、情報信号に重畳された情報である。

【0046】また、アナログ入力端子302を通じて入

力された映像情報は、アナログ入力端子302を通じてエンコード部304に供給され、MPEG圧縮される。その結果、圧縮映像データが生成される。この際、入力された情報信号が複製可能であるかどうかを示す複製制御情報を検出する。

【0047】セレクト305はユーザの入力選択に応じたセレクト制御信号により、暗号解読部303からのデータと、エンコード部304からのデータとのいずれかを選択して出力する。

【0048】このセレクト305から出力されるデータは、WM書換部306を介して記録制御部308に供給される。WM書換部306は、電子透かし情報として情報信号にスクランブル情報“Scrambled (RAM)”を重畳するための処理を行う。ただし、この処理は後に説明する記録媒体の種別の判別を行った上で行う必要がある。WM書換部306の処理は、例えば、擬似雑音符号系列の符号を用いてスクランブル情報をスペクトラム拡散し、スペクトラム拡散したスクランブル情報を出力する。これは周知の技術であるから、詳細な説明は省略する。セレクト305から出力されるデータは、WMデコード部307にも供給される。WMデコード部307は、電子透かし情報として情報信号に重畳されているスクランブル情報の抽出、記述内容の判別を行い、判別出力をコントロール部309に供給する。

【0049】コントロール部309は入力情報から検出された複製制御情報および電子透かし情報の判別出力に基づいて、入力情報の記録（複製）が可能であるか否かの判別を行い、記録（複製）可能であると判別した場合は、さらに、複製制御のために電子透かし情報の書換えが必要であるか否かを判別する。そして記録禁止と判別したときには、コントロール部309は、記録制御部308が記録を実行しないよう制御する。また、記録可能、または、1回複製可能と判別したときには、コントロール部309は記録制御部308に記録を実行させる。このとき、記録装置102は、読み出し部313を介してディスクの種別（RAMディスク、1回のみ書き込み可能なディスク等のタイプ）に関する情報を読み出し、ディスク種別判別部314でそのディスクの種別を判別する。その結果、先に説明したようなスクランブル情報の内容が決定され、WM書き換え部306において情報信号に重畳すべきスクランブル情報が生成され、記録制御部308において情報信号に重畳される。情報信号は、スクランブル部310によりそのディスクの種別に応じた特定のスクランブルを施され、書き込み部311を介してRAMディスク312に記録される。

【0050】次に図4を参照して、コンプライアント記録装置102が暗号解読を終了した後の処理を説明する。図4は、記録装置102の記録処理フローを示すフローチャートである。

【0051】まず、情報信号が入力された時に検出した

複製制御情報をチェックする(ステップS101)。そして、複製制御情報が“Never Copy”(絶対複製禁止)または、“No More Copy”(これ以上複製禁止)であるか否かを判別する(ステップS102)。いずれかに該当する場合には、記録を禁止し、記録処理を中止する(ステップS103)。なお“Never Copy”(絶対複製禁止)とは、情報信号の複製が全く禁止されるという制限が課されることを表す。一方、“No More Copy”(これ以上複製禁止)は、1回だけ複製可能な音楽データや画像データが複製された場合に、これ以上の情報信号の複製が禁止されるという制限が課されることを表す。いずれにも該当しない場合(“Never Copy”または“No More Copy”でない場合)には、入力信号に重畳されている電子透かし情報(WM)の判定出力をチェックし(ステップS104)、電子透かし情報(WM)が“Scrambled”の状態であるかどうかを判別する(ステップS105)。“Scrambled”の状態であれば、記録しようとしている情報信号は元々スクランブルされていた情報であることから、この情報信号が複製制御情報を不正に改竄して入力された情報であると判断し、記録処理を中止する(ステップS103)。“Scrambled”の状態でなければ、記録可能な情報であると判断できる。

【0052】記録可能な情報であると判断すると、次にその情報信号をスクランブルする必要があるか否かを判断するために、複製制御情報が“1回複製可能(One Copy)”の状態にある情報信号か否かを判別する(ステップS106)。“1回複製可能”の状態にある場合は、電子透かし情報を“Scramble(RAM)”状態に書き換え(ステップS107)、特定のスクランブル方式に従ったスクランブル処理を実施する(ステップS108)。記録装置102(図3)は、このようにして生成した情報をRAMディスクに記録する(ステップS109)。

【0053】“1回複製可能”ではない場合(何度でも“複製可能”の場合)は、スクランブル処理を行わずRAMディスクに記録する(ステップS109)。

【0054】以上のようなコンプライアント記録装置102によって記録されたRAMディスクは、複製制御が必要な“1回複製可能”な情報信号に対して、電子透かし情報としてのスクランブル情報と情報信号に対するスクランブルが対となって記録される。

【0055】さらに、読み出し部213(図2)が読み出した所定の情報に基づいて、ディスク種別判別部214が装填されたディスクの種別を判別し、電子透かし情報にディスク種別を記録してもよい。ディスク種別は、ROMディスク(再生専用)であるか、RAMディスク(書込可能)であるか、さらには、1回書き込みのみ可能なディスクであるか、1000回程度書き込み可能なディスクか、10万回程度書き込み可能なディスクであ

るか等である。ディスクの判別は、例えば、ディスクの物理特性(フォーカス特性、トラッキング特性、再生特性)やディスク種別を記録したコントロール領域の情報等に基づいて行われる。

【0056】なお、スクランブル処理に関しては、情報再生時の負荷を考慮し、一部の情報のみ(MPEG圧縮データのIフレームデータなど)をスクランブル対象としてもよい。この場合、電子透かし情報は、当該一部の情報全てに重畳する必要が生じる。

【0057】なお、上記のような情報信号をスクランブルしたROMディスクを制作するような場合には、例えば、情報記録装置がオーサリングシステムとディスクカッティングシステムとして構成される。オーサリングシステムは、情報信号に応じて情報信号の圧縮処理を行うとともに、電子透かし情報としてスクランブル情報を重畳する。ディスクカッティングシステムは、情報信号に応じてスクランブル処理を施し、ディスク原盤を作成する。これらを用いれば、上述したような複製制御が可能なROMディスクを制作できる。

【0058】[再生装置]次に図5を参照して、コンプライアント再生装置105の構成を説明する。なおコンプライアント再生装置105とコンプライアント再生装置101とは同じ構成である。図5は、コンプライアント再生装置105の構成を示すブロック図である。再生装置105に装填されたディスクに記録されている情報は、読み出し部401で読み出され、デスクランブル部402、スクランブル状態検出部403、ディスク種別判別部404に供給される。

【0059】スクランブル状態検出部403は、付加情報としてディスクに記録されているスクランブルフラグを抽出して、記録情報にスクランブルがかかっているか否かを検出し、その検出結果をコントロール部405に出力する。なお、複製禁止のROMディスクには、特定暗号方式(例えば、CSS: Contents Scramble System方式など)の暗号がかけられているものとする。

【0060】ディスク種別判別部404は、装填されたディスクの種別を判別し、その判別結果をコントロール部405に供給する。ディスク種別は、ROMディスク(再生専用)であるか、RAMディスク(書込可能)であるか、さらには、1回書き込みのみ可能なディスクであるか、1000回程度書き込み可能なディスクか、10万回程度書き込み可能なディスクであるか等である。ディスクの判別は、例えば、ディスクの物理特性(フォーカス特性、トラッキング特性、再生特性)やディスク種別を記録したコントロール領域の情報等に基づいて行われる。

【0061】デスクランブル部402は、ROMディスクの場合には製造元に施されたスクランブルを、RAMディスクの場合には記録装置のスクランブル部240

(図2の(b))で施されたスクランブルを解説する。デスクランブル部402は、図2の(a)を参照して説明したデスクランブル部220の処理を行う。

【0062】デスクランブル部402は、WMデコード部406と再生制御部407に出力したデータを供給する。WMデコード部406は、電子透かし情報として情報信号に重畳されているスクランブル情報を復号化する。「復号化」とは、スクランブル情報を抽出し、その内容を判別することを表す。これは、電子透かし情報は雑音として情報信号に重畳されており、符号化されていると考えられるからである。WMデコード部406は、判別結果をコントロール部405に出力する。

【0063】コントロール部405は、これらのディスク種別の判別結果、スクランブルフラグ、および電子透かし情報の判別出力に基づいて、再生を許可するか、禁止するかを決定する。コンプライアント記録装置102(図1)が記録したディスクでは、情報信号に対するスクランブルとスクランブル情報が表す内容とが対になるように記録されている。

【0064】よってこれに違反するようなディスクが装填された場合には、デスクランブル部402は、再生禁止の制御情報を再生制御部407に供給して、この再生制御部407以降の処理を禁止する。正規のディスクからの情報信号の場合には、再生制御部407以降の処理が有効となる。再生制御部407は映像音声情報をデコード部408に供給し、デコード部408はMPEG圧縮されていたデータを伸長(デコード)する。アナログI/F409は、伸長(復号)されたデータをD/A変換し、外部の機器に供給する。また、デジタルI/F411に接続される機器がある場合には暗号化部410はMPEG圧縮されたデータを暗号化し、デジタルI/F411から出力する。

【0065】次に図6を参照して、コンプライアント再生装置105(図5)の再生処理を説明する。図6は、再生処理フローを示すフローチャートである。再生装置105(図5)では、まず装填されたディスクに記録されている情報信号に、スクランブルがかかっているかを判別する(ステップS201)。スクランブルには、記録装置102のスクランブル部240(図2)でかけられるRAMディスク用のスクランブル方式のものと、ROMディスク用のスクランブル(例えば、CSS方式)がある。ディスクの種別に応じてスクランブルの方式も異なるため、ディスク種別判別部404(図5)はディスク種別をチェックする(ステップS202)。

【0066】ディスク種別のチェックの結果、ディスクがROMディスクである場合、デスクランブル処理部402(図5)はROM用のデスクランブル処理を行う(ステップS203)。次にWMデコード部406(図5)は、デスクランブルされた情報信号にスクランブル状態を示す電子透かし情報(WM)が記述されているか

否かをチェックし(ステップS204)、コントロール部405(図5)は、電子透かし情報が“Scrambled(ROM)”の状態であるかどうかを判別する(ステップS205)。“Scrambled(ROM)”の状態であるときには、コントロール部405(図5)は再生を許可し(ステップS211)、その状態にない時には再生を禁止する(ステップS212)。

【0067】ステップS202におけるディスク種別のチェックの結果、ディスクがRAMディスクである場合も同様に、デスクランブル処理部402(図5)はRAM用のデスクランブル処理を行う(ステップS206)。そしてWMデコード部406(図5)は、スクランブル状態を示す電子透かし情報(WM)をデスクランブルされた情報信号から検出し(ステップS207)、コントロール部405(図5)は、電子透かし情報が“Scrambled(RAM)”の状態であるかどうかを判別する(ステップS208)。“Scrambled(RAM)”の状態であるときには、コントロール部405(図5)は再生を許可し(ステップS211)、その状態にない時には再生を禁止する(ステップS212)。

【0068】また、ステップS201でスクランブルがかかっていないと判断された場合には、デスクランブル部402(図5)はデスクランブル処理を行うことなく、信号情報をWMデコード部406(図5)に送信する。WMデコード部406(図5)は、電子透かし情報(WM)を検出し(ステップS209)、コントロール部405(図5)は電子透かし情報が“Scrambled”の状態であるかどうかを判別する(ステップS210)。“Scrambled”の状態にあるときは、コントロール部405(図5)は再生を禁止(ステップS212)し、その状態でないときは、再生を許可(ステップS211)する。ここでいう「その状態でないとき」とは、電子透かし情報が検出されないとき、または、検出された電子透かし情報が“Non-Scrambled”のときである。

【0069】すなわち、コンプライアント記録装置102(図1)で記録されたディスクであれば、電子透かし情報WMが“Scrambled”と記録されている情報信号には、スクランブル処理が行われている。しかし、電子透かし情報WMに“Scrambled”と記録されているにもかかわらず情報信号がスクランブルされていないということは、その情報信号は不正に複製されたことを意味する。例えば、コンプライアント再生装置101(図1)の出力がノンコンプライアント記録装置103(図1)によりディスクに記録された場合、または、情報信号に施されているスクランブルを不正にデスクランブルし、ディスクに記録した場合が該当する。

【0070】一方、上記のような本発明による記録装置102(図1、図3)ならびに再生装置101、105

(図1、図5)を用いれば、このような場合の再生を禁止することができる。これにより、再生装置に電子透かし情報を書き換えるための書換手段を実装しなくとも、不正な複製の防止が可能であり、再生装置のコストダウンが容易となる。

【0071】なお、一部の情報信号のみがスクランブルされているような場合には、情報信号のスクランブルフラグのみではなく、デスクランブル部402においてデスクランブル処理が正常に行われたかどうかをチェックすることが必要である。これにより、不正に複製した情報信号のスクランブルフラグをスクランブル状態に書き換えるといった不正に対しても、再生を禁止することが可能となる。ここでは、スクランブルにより情報信号に対する暗号化を行ったが、他の方式を用いて暗号化を行った場合も同様の効果が得ることができる。

【0072】なお、実施の形態1では、光ディスクを情報記録媒体として用いた場合について説明したが、他の半導体メモリや磁気記録媒体（ハードディスクなど）についても同様である。

【0073】（実施の形態2）実施の形態1では、記録装置102（図1、図3）および再生装置101、105（図1、図5）は、ディスクへの情報信号の記録、または、ディスクからの情報信号の再生を行うブロック（書き込み部311（図3）、読み出し部401（図5））、電子透かし情報を検出するブロック（WMデコード部307（図3）、406（図5））、情報信号を伸長／圧縮するブロック（エンコード部304（図3）、デコード部408（図5））とを、装置内部にすべて含むよう構成されているとして説明した。

【0074】ところが、PCで記録装置や再生装置の機能を実現する場合には、情報信号の記録・読み出しを行うドライブ部と、エンコーダ／デコーダ部とがそれぞれ別個の装置として構成されるのが一般的である。

【0075】別個の装置として構成した場合、ドライブ部で検出したディスク種別に基づいてデコーダ部が再生制御を行うため、ディスク種別が不正にすり替えられ不正に複製したディスクが再生可能となってしまう。具体的に説明すると、ROMディスクに記録された情報信号をノンコンプライアント記録装置によりRAMディスクに記録し、その後再生する場合には、ドライブ部とデコーダ部の間で不正なソフトウェアが介在することで、ドライブの検出したディスク種別を“ROM”とすりかえることが可能である。この結果、ROMディスクをRAMディスクへ不正複製した場合にコンプライアント再生装置101、105（図1）のように再生を防止できなくなる。本実施の形態は、このような場合でも再生を防止する構成を説明する。

【0076】【PCによる記録装置】図7は、パーソナルコンピュータ（PC）記録システム600によりコンプライアント記録装置を実現した例を示す図である。図

7に示すように、このようなコンプライアントなPC記録システム600は、主にPCエンコーダ600-1とPC記録装置（ドライブ）600-2とから構成されており、それらの間は、不正な複製を防止可能なデジタルI/F（SCSIやATAPI、IEEE1394等）で接続されている。PCエンコーダ600-1は、コンプライアント記録装置102（図3）のI/F301、302（図3）からスクランブル部310（図3）までの構成に相当し、その動作と同じ動作を行う。したがって共通の動作に関する説明は省略する。一方、PC記録装置（ドライブ）600-2は、書き込み部311（図3）の構成に相当する。

【0077】以下、PCエンコーダ600-1の動作が、コンプライアント記録装置102（図3）のI/F301、302（図3）からスクランブル部310（図3）までの構成により実現される動作と異なる点を説明する。1回複製可能な情報信号をRAMディスクに記録する場合には、PCエンコーダ600-1のスクランブル部610は、その情報信号に特定のスクランブルを施す。この際、スクランブルの基となる鍵情報をPC記録ドライブとPCエンコーダ間で安全に共有するために、デジタルI/F615、616を介して認証部613、617が相互認証を行う。認証が成立した場合には、認証部613とPC記録ドライブ中の認証部617との間でお互いが正規のライセンスを受けた装置、すなわちコンプライアントな装置であることを確認できる。認証が成立した場合は、さらにデジタルI/F上に伝送するデータを暗号化するためのバス鍵を共有する。このようにして、共有化されたバス鍵を用いて、PCエンコーダでは、暗号化部614において保護が必要なデータ（鍵情報や情報信号など）を暗号化し、デジタルI/F615を介して暗号化されたデータをPC記録ドライブ600-2に送信する。

【0078】PC記録ドライブ600-2の暗号解読部618は、共有化したバス鍵に基づいて受信したデータを復号する。書き込み部611は、PCエンコーダ600-1から受信した情報信号をRAMディスク612に記録する。このとき記録制御部619は、PCエンコーダに対する認証が成立していない限り、鍵情報等の特定の保護領域に記録する必要があるデータをRAMディスク612に書き込まないよう記録制御する。

【0079】コンプライアントな装置では、ディスク種別や記録されている情報信号によって、相互認証の方式や鍵情報と情報信号に対する処理方法を変化させている。PCドライブ600-2のディスク種別判別部621は、読み出し部620から再生された信号に基づいて、ディスク612の物理特性（フォーカス特性、トラッキング特性、再生特性）や、ディスク612のコントロール領域に記録されたディスク種別を判別する。判別結果は、コントロール部622に出力される。なお、デ

ィスク種別を表す情報が転送中に改竄される可能性がある。しかし後述の手法によれば、そのような転送中の改竄を防止できる。コントロール部622では、ディスク種別にあわせて認証方式、データの伝送方式などを切り替え、PCエンコーダ600-1とデータ伝送を行う。

【0080】次に、PC記録システム600のPCエンコーダ600-1およびPCドライブ600-2の処理の流れを説明する。図8は、PCエンコーダ600-1のコントロール部609(図7)における処理フローを示すフローチャートである。まず、1回複製可能な情報信号を記録する場合、コントロール部609(図7)は、認証部613とPCドライブ600-2の認証部617(図7)との間で相互に認証を行わせる(ステップS301)。認証部613(図7)による認証の結果、コントロール部609(図7)は、双方がコンプライアント装置であるか否かを判別する(ステップS302)。これにより、情報信号の記録に先立って正規にライセンスを受けた機器であるか否かを確認できる。

【0081】認証が成立した場合は、PCエンコーダ600-1とPCドライブ600-2(図7)との間で共通のバス鍵を生成する(ステップS303)。そしてPCエンコーダ600-1(図7)は、PCドライブ600-2(図7)で生成されたスクランブルに用いる鍵情報(以下、「スクランブル鍵情報」と称する)をPCドライブ600-2から取得する(ステップS304)。スクランブル鍵情報は、共有したバス鍵に基づいてPCドライブ600-2が暗号化および/または改竄防止処理を施し転送した情報である。

【0082】PCエンコーダ600-1のコントロール部609(図7)では、図4と同様の記録フローにしたがって情報信号の記録を行う(ステップS305以降のステップ)。この記録フローは図4を参照して既に説明したので、その説明は省略する。

【0083】図4のフローとの相違点は、ステップS106(図4)の“1回複製可能”の判別後に、相互認証が成立しているか否かのチェックを行うステップS311が挿入されていることである。ステップS311において相互認証が成立していない場合は、記録禁止とされる。

【0084】続いてPCドライブ600-2(図7)の処理を説明する。図9は、PC記録ドライブ600-2のコントロール部622(図7)における処理フローを示すフローチャートである。先のPCエンコーダ600-1と同様、1回複製可能な情報信号を記録する場合、コントロール部622(図7)は認証部617(図7)とPCエンコーダ600-1の認証部613(図7)との間で相互に認証を行わせる(ステップS401)。そして認証部617(図7)による認証の結果、コントロール部622(図7)は、相互認証が成立したか否かを判別する(ステップS402)。

【0085】認証が成立した場合は、コントロール部622(図7)は共通なバス鍵を生成する。そしてコントロール部622(図7)は、共有したバス鍵に基づいてスクランブル鍵情報に暗号化および/または改竄防止処理を施し、PC記録ドライブ600-2(図7)からPCエンコーダ600-1(図7)に転送を行う(S404)。そして、スクランブルされた情報信号、ならびにスクランブル鍵情報やスクランブル制御情報等へのアクセス(記録や再生)を許可し、記録が行われる(ステップS405)。一方、ステップS402において相互認証が成立しない場合は、情報信号のみの記録を許可し、ディスクの一部の特定領域へのスクランブル鍵情報、スクランブル制御情報等の記録を禁止する。(ステップS406)。

【0086】したがって、コンプライアントなPCエンコーダ600-1およびPCドライブ600-2(図7)同士でない場合には、スクランブル鍵情報やスクランブル制御情報等へのアクセスが防止できる。この結果、複製制御が必要な1回複製可能な情報信号の記録において、双方がコンプライアントなPCエンコーダ600-1とPCドライブ600-2とを組み合わせたコンプライアントPCシステム600(図7)では、電子透かし情報“Scrambled”と情報信号に対するスクランブル状態とが検出され、複製が可能となる。一方、PCエンコーダとPCドライブのいずれかがノンコンプライアントなPCシステムでは、ディスク上の特定領域へのアクセスができず、正しいスクランブルの実施ができない。

[PCによる再生装置] 図10は、パーソナルコンピュータ(PC)再生システム900によりコンプライアント再生装置を実現した例を示す図である。図10に示すように、このようなコンプライアントなPC再生システム900は、主にPCデコーダ900-1とPC再生装置(ドライブ装置)900-2とから構成されており、それらの間は、不正な複製を防止可能なデジタルI/F(SCSIやATAPI, IEEE1394等)で接続されている。PCデコーダ900-1は、コンプライアント再生装置101、105(図5)のデスクランブル部402(図5)からI/F409、411(図5)までの構成に相当し、その動作と同じ動作を行う。したがって共通の動作に関する説明は省略する。一方、PC再生装置(ドライブ)900-2は、読み出し部401(図5)の構成に相当する。読み出し部901は、このPC再生装置(ドライブ)900-2に装填されたディスク950から、記録されている情報を読み出し、スクランブル状態検出部904、ディスク種別判別部903に供給する。スクランブル状態検出部904、ディスク種別判別部903は、コンプライアント再生装置101、105(図5)の場合と同様に、スクランブルフラグおよびディスク種別を得る。

【0087】PC再生装置(ドライブ)900-2の認証部915は、スクランブルが施されている情報信号をデジタルI/F916から出力する場合、PCデコーダ900-1の認証部919との間で相互認証を行う。認証が成立していない場合には、再生制御部913がPC再生ドライブからの情報信号の読み出しを禁止する。認証が成立した場合には、PCデコーダ中のデスクランブル部902は、情報信号を読み出し、スクランブルが施された複製禁止の情報信号に特定のデスクランブル処理を施す。

【0088】この際、スクランブルの基となる鍵情報をPC再生ドライブとPCデコーダ間で安全に共有するために、デジタルI/F916、917を介して認証部915、919が相互認証を行う。認証が成立した場合には、認証部915と認証部919との間でお互いが正規のライセンスを受けた装置であることを確認できる。具体的には、正常に認証が成立した場合は、さらにデジタルI/F上に伝送するデータを暗号化するためのバス鍵を共有する。このようにして、共有化されたバス鍵を用いて、PC再生装置(ドライブ)900-2では、暗号化部914において保護が必要なデータ(鍵情報や情報信号など)を暗号化し、デジタルI/F916を介して暗号化されたデータをPCデコーダ900-1に送信する。

【0089】コンプライアントな装置では、ディスク種別や記録されている情報信号によって、相互認証の方式や鍵情報と情報信号に対する処理方法を変化させている。ディスク種別判別部903は、読み出し部901の再生信号に基づいて物理特性(フォーカス特性、トラッキング特性、再生特性)やディスク種別を記録したコントロール領域などから判別を判別する。判別結果は、コントロール部912に出力される。コントロール部912では、ディスク種別にあわせて認証方式、データの伝送方式などを切り替え、PCデコーダ900-1とのデータ伝送を行う。PCデコーダ900-1でも同様に、再生する情報信号が記録されたディスク種別や情報信号のスクランブル方式に合わせて認証方式、データの伝送方式などを切り替える。

【0090】PCデコーダ900-1の暗号解読部918は、共有化したバス鍵に基づいて受信したデータを復号する。デスクランブル部902からI/F部909、911までの処理は、コンプライアント再生装置101、105(図5)の場合と同様であるのでその説明は省略する。

【0091】PCデコーダ900-1のコントロール部905は、情報信号のスクランブル(スクランブルの有無やスクランブル方式)、電子透かし情報としてのスクランブル情報による再生制御のみではなく、認証方式やデータ伝送方式等も利用して再生制御を行う。

【0092】次に、PC記録システム900のPCデコ

ーダ900-1およびPC再生装置(ドライブ)900-2の処理の流れを説明する。図11は、PCドライブ900-2のコントロール部912(図10)における処理フローを示すフローチャートである。まず、ディスク上にスクランブルされて記録されている情報信号を再生する場合、コントロール部912(図10)は、認証部915と、PCエンコーダ600-1の認証部919との間で相互に認証を行わせる(ステップS501)。認証部915による認証の結果、コントロール部912(図10)は、双方がコンプライアント装置であるか否かを判別する(ステップS502)。これにより、情報信号の記録に先立って正規にライセンスを受けた機器であるか否かを確認できる。

【0093】認証が成立した場合は、PCデコーダ900-1とPCドライブ900-2(図10)との間で共通のバス鍵を生成する(ステップS503)。そしてコントロール部912(図10)は、共有したバス鍵に基づいてスクランブル鍵情報に暗号化および/または改竄防止処理を施し、PCドライブ900-2(図10)からPCデコーダ900-1(図10)に転送を行う(S504)。そして、スクランブルされた情報信号、ならびにスクランブル鍵情報やスクランブル制御情報等へのアクセスを許可し、再生が行われる(ステップS505)。一方、ステップS502において相互認証が成立しない場合は、情報信号のみの再生を許可し、ディスクの一部の特定領域の情報の再生を禁止する。(ステップS506)。

【0094】図12は、PCデコーダ900-1のコントロール部905(図10)の処理フローを示すフローチャートである。先のPCドライブ900-2と同様、ディスク上にスクランブルされて記録されている情報信号を再生する場合、コントロール部905(図10)は、認証部919、認証部915との間で相互に認証を行わせる(ステップS601)。そして認証部919による認証の結果、コントロール部905(図10)は、相互認証が成立したか否かを判別する(ステップS502)。

【0095】認証が成立した場合は、PCデコーダ900-1とPCドライブ900-2(図10)との間で共通のバス鍵を生成する(ステップS603)。そしてPCデコーダ900-1(図10)は、PCドライブ900-2(図10)で生成されたスクランブル鍵情報をPCドライブ900-2から取得する(ステップS604)。

【0096】PCデコーダ900-1のコントロール部905(図10)では、図6と同様に示した再生フローにしたがって情報信号の再生を行う(ステップS605以降のステップ)。この再生フローは図6を参照して既に説明したので、その説明は省略する。

【0097】図6のフローとの相違点は、ステップS2

02 ( 図6 ) のディスク種別の判別後に、それぞれのディスクに対応した相互認証が成立しているか否かのチェックを行うように変更されていることである ( ステップ S609、S612 ) 。 ROM または RAM 用の相互認証が成立していない場合は、このような情報信号の再生禁止とされる。

【0098】したがって、コンプライアントな PC デコーダ 900-1 および PC ドライブ 900-2 ( 図10 ) 同士でない場合には、スクランブル鍵情報やスクランブル制御情報等へのアクセスが防止できる。この結果、複製制御が必要な複製不可能な情報信号の再生において、双方がコンプライアントな PC デコーダ 900-1 および PC ドライブ 900-2 ( 図10 ) とを組み合わせた PC 再生システム 900 ( 図10 ) では、情報信号に対するデスクランブル状態と電子透かし情報 “Scrambled” とが検出される。ノンコンプライアント PC システムではディスク上の特定領域からの鍵情報の再生ができず、正規のデスクランブルを防止できる。

【0099】〔ディスク種別転送方式〕次に図13を参照して、ディスク種別を改竄されることなく PC ドライブ部からエンコーダやデコーダに転送する方法を詳細に説明する。図13は、ディスク種別の情報を転送する際のデータの流れを示す図である。PC ドライブ部は、PC ドライブ 600-2 ( 図7 ) または PC ドライブ 900-2 ( 図10 ) である。

【0100】PC エンコーダまたは PC デコーダでは、ディスク種別を利用して情報信号の記録再生を許可する。このため、ディスク種別を表す情報を、ドライブ部からエンコーダ部またはデコーダ部に改竄されることなく転送することが必要である。PC エンコーダまたは PC デコーダは、例えば、PC エンコーダ 600-1 ( 図7 ) または PC デコーダ 900-1 ( 図10 ) である。

【0101】図13のディスク1250には、ドライブ部とエンコーダ/デコーダ間の相互認証に使用する認証鍵情報1201が記録されている。認証鍵情報1201は、1または複数の暗号化認証鍵 ( EAK1、EAK2、・・・ ) の集合である。暗号化認証鍵は、相互認証に使用する共通鍵 ( 認証鍵 ) と認証鍵情報が記録されるディスクの種別とが、デバイス鍵で暗号化された鍵である。デバイス鍵は、個々の装置に割り当てられた鍵である。

【0102】暗号化認証鍵の例を以下に示す。

【0103】 $EAK1 = ENC ( \text{デバイス鍵} ( DK1 ), \{ \text{認証鍵} ( AK ), \text{ディスク種別} ( DT ) \} )$

$EAK2 = ENC ( \text{デバイス鍵} ( DK2 ), \{ \text{認証鍵} ( AK ), \text{ディスク種別} ( DT ) \} )$

PC ドライブの認証部 915 は、ディスク1250 から読み出した認証鍵情報から機器に割り当てられた暗号化認証鍵 ( EAK1 ) を取り出し、自己が保有しているデバイス鍵 DK1 で復号する。この結果、認証鍵と ( A

K ) ディスク種別 ( DT ) が得られる。PC ドライブは、装填されたディスクの物理特性 ( フォーカス特性、トラッキング特性、再生特性 ) やディスク種別を記録したコントロール領域等からディスク種別 ( DT' ) を判別する。相互認証は、認証鍵 ( AK ) とディスク種別判別部1202からのディスク種別 ( DT' ) とを特定の演算 ( 例えば、図では加算 ) によって得られたディスク認証鍵 ( DAK' ) を用いる。

【0104】一方、PC エンコーダ/PC デコーダでは、ディスク1250 から読み出した認証鍵情報から機器に割り当てられた暗号化認証鍵 ( EAK2 ) を取り出し、自己が保有しているデバイス鍵 DK2 で復号する。この結果、認証鍵と ( AK ) ディスク種別 ( DT ) が得られる。相互認証には、認証鍵 ( AK ) とディスク種別 ( DT ) とを特定の演算 ( 例えば、図では加算 ) によって得られたディスク認証鍵 ( DAK ) を用いる。

【0105】このようにして共有化したディスク認証鍵を用いて相互認証を行う。すなわち、 $DAK = DAK'$  の場合は相互認証が成立し、 $DAK \neq DAK'$  の場合は相互認証が成立しない。つまり、認証部 915 および 919 は、認証鍵情報の DT とドライブが検出した DT' が一致しない時には、認証を不成立にできる。この結果、ROM ディスクから入手した情報信号や鍵情報を RAM ディスクに不正に複製したとしても、認証鍵情報中のディスク種別 ( DT ) とドライブが検出するディスク種別 ( DT' ) とは不一致となる。よって相互認証が成立せず、情報信号の再生を防止できる。また、認証鍵情報を不正にすりかえたとしても、認証鍵やディスク種別が不一致となり、相互認証が不成立となる。

【0106】なお、認証鍵情報に認証鍵とディスク種別を暗号化して記録した場合を説明した。しかし、認証鍵情報にディスク種別を含めず、ドライブで検出したディスク種別を暗号化して PC エンコーダやデコーダに伝送し、復号してディスク種別を得る方法であっても、ディスク種別を安全に転送することができる。よって実質的に正常な情報信号の再生は可能である。認証鍵情報にディスク種別を含めない場合には相互認証がディスクの種別によらず共通になり、ディスク種別によらず相互認証は成立する。ただし相互認証は成立していても、誤ったディスク種別 ( スクランブル方式 ) で情報信号が再生される場合には映像や音声が表示されなくすることもできる。

【0107】上記のような記録装置または再生装置によると、PC ドライブ部に WM 検出部や WM 書換部を実装しなくても、不正な複製ディスクの再生を防止できる。

【0108】次に、ディスク種別によって認証方式やデータの伝送方式 ( データや鍵情報の伝送手順 ) を変化させる処理を説明する。この性質を逆に利用すれば、認証を行った処理手順からディスク種別の判別を行う処理も可能である。以下の説明は、( 図10 ) PC ドライブと

PCデコーダとして利用可能なシステムである。

【0109】図14は、再生システム1400がDVD-ROMディスク1450を再生する場合の認証手順とデータ転送手順を示す。まずバス認証ステップを説明する。MPEGデコーダモジュール1428が乱数 $c1$ を生成し、チャレンジデータ( $drv\_chal(c1)$ )としてDVDドライブ1400-1にセットする。DVDドライブ1400-1は、秘密情報である関数 $f$ を用いて $f(c1)$ を生成し、レスポンスデータ( $drv\_res(f(c1))$ )としてMPEGデコーダモジュール1400-2に返す。MPEGデコーダモジュール1400-2は、自らが有する秘密情報である関数 $f$ を用いて $f(c1)$ を生成する。そしてMPEGデコーダモジュール1400-2は、 $f(c1)$ がDVDドライブ1400-1から返されたレスポンスデータと一致しているかどうかをチェックし、MPEGデコーダ1428はDVDドライブ1400-1がコンプライアントな機器であることを確認する。

【0110】次に、DVDドライブ1400-1が乱数 $c2$ を生成し、チャレンジデータとしてMPEGデコーダモジュール1400-2にセットする( $dec\_chal(c2)$ )。MPEGデコーダモジュール1400-2は、秘密情報である関数 $f$ を用いて $f(c2)$ を生成し、レスポンスデータとしてDVDドライブ1400-1に返す( $dec\_res(f(c2))$ )。DVDドライブ1400-1は、自らが有する秘密情報である関数 $f$ を用いて $f(c2)$ を生成する。そしてDVDドライブ1400-1は、 $f(c2)$ がMPEGデコーダモジュール1400-2から返されたレスポンスデータと一致しているかどうかをチェックし、DVDドライブはMPEGデコーダがコンプライアントな機器であることを確認する。この結果、DVDドライブ1400-1とMPEGデコーダモジュール1400-2の間で秘密の時変鍵が共有される。

【0111】続いて時変鍵を用いた鍵情報の秘密伝送ステップを説明する。DVDドライブ1400-1は、共有した時変鍵を用いてDVD-ROMディスク1450に記録された暗号化ディスク鍵セットと暗号化タイトル鍵をバス暗号化し、MPEGデコーダモジュール1400-2に転送する。MPEGデコーダモジュール1400-2では、受け取ったバス暗号化された暗号化ディスク鍵セットと暗号化タイトル鍵を、共有した時変鍵を用いてバス復号化する。

【0112】スクランブルされた情報信号の復号に関して、MPEGデコーダモジュール1400-12は、バス復号化された暗号化ディスク鍵セットと暗号化タイトル鍵を利用して、図2の(a)に示すようにスクランブルされた情報信号を復号して、コンテンツとしての情報信号を得ることができる。

【0113】図15は、再生システム1500がDVD-Rディスク1550を再生する場合の認証手順とデータ転送手順を示す。まずバス認証ステップは、上述のD

VD-ROM1450(図14)ディスクを再生する場合のバス認証ステップと同じである。したがってその説明は省略する。次に時変鍵を用いた鍵情報の秘密伝送ステップを説明する。DVDドライブ1500-1は、共有した時変鍵を用いて暗号化ディスク鍵セットをバス暗号化し、メディアIDに改ざんチェックコードを付与する。そしてDVDドライブ1500-1は、暗号化ディスク鍵セットとメディアIDとをMPEGデコーダモジュール1500-2に転送する。MPEGデコーダモジュール1500-2は、受け取ったバス暗号化された暗号化ディスク鍵セットを、共有した時変鍵を用いてバス復号化する。またMPEGデコーダモジュール1500-2では、メディアIDに付与されている改ざんチェックコードを、共有した時変鍵を用いてチェックする。

【0114】最後にスクランブルされた情報信号(コンテンツ)の復号を説明する。MPEGデコーダモジュール1500-2は、DVD-Rディスク1550のユーザ領域から暗号化タイトル鍵とスクランブルされた情報信号(AVデータ)を読み出す。そしてMPEGデコーダモジュール1500-2は、復号化された暗号化ディスク鍵セットでディスク鍵を復号し、そのディスク鍵でディスク固有鍵を復号する。さらにそのディスク固有鍵でタイトル鍵を復号し、そのタイトル鍵でスクランブルされた情報信号をデスクランブルする。

【0115】上記のように、スクランブルされた情報信号の復号に必要な鍵等の情報は、再生型DVD(DVD-ROMディスク)と記録型DVD(DVD-Rディスク)とで異なるので、転送されるデータや転送手順が異なる。本発明は、DVDドライブでディスク種別を識別し、それに対応した転送手順に従うように制御する。MPEGデコーダモジュールでは、データ転送手順の違いからディスク種別を識別し、電子透かし情報に重畳されているディスク種別と一致比較することによって、再生制限を行うことができる。なお図14および図15では、再生型DVDと記録型DVDとで同じ認証方法を用いている。しかし再生型DVDと記録型DVDとで異なる認証方法を用いることで、認証方法の相違からMPEGデコーダモジュールは上記の場合と同様にディスク種別を識別できる。異なる認証方法としては、異なるアルゴリズム(上記関数 $f$ )を使用する認証方法、および、同一のアルゴリズムであってもアルゴリズム中で異なるパラメータを使用するなどがある。これまでの説明では、スクランブルにより情報信号に対する暗号化を行ったが、他の方式を用いて暗号化を行った場合も同様の効果が得ることができる。

【0116】本実施の形態では、光ディスクを情報記録媒体として用いた場合について説明した。しかしその説明は、他の半導体メモリや磁気記録媒体(ハードディスクなど)についても同様の方法で適用可能である。また、本発明の暗号化された情報信号は、インターネット

等のネットワーク回線（伝送媒体）や、デジタル放送等の番組として電波で伝送されてもよい。このとき上述した認証手順により、受信側と送信側とで認証を行うことで、不正な複製を防止できる。

#### 【0117】

【発明の効果】以上説明したように、本発明によれば、所定の複製制御の対象となる情報信号（例えば、これ以上複製禁止、または、絶対複製禁止の情報信号）に対しては、当該情報信号がスクランブルされていることを示すスクランブル情報を電子透かし情報として重畳し、かつ、情報記録媒体の種別にしたがったスクランブルを行って情報記録媒体への記録を行うようにした。これにより、スクランブルを解読した後の情報記録媒体への不正な記録や、不正に複製した他の種類の情報記録媒体からの再生を制限できる。後者についてより具体的には、情報再生装置は、読み出した情報信号に重畳されている電子透かし情報（スクランブル情報）の示す状態と、読み出した情報信号のスクランブル状態（スクランブルされているか否か）を比較する。これにより、比較結果が不一致の場合には、不正な複製によって作成された情報記録媒体からの再生であるとして、その再生を防止できる。なお本発明によれば、情報再生装置において電子透かし情報の書き換えは行わないので、電子透かし情報の書換手段を実装する必要がなく、安価な構成をとることができる。

#### 【図面の簡単な説明】

【図1】 実施の形態1による複製世代管理方法を説明するための概略図である。

【図2】 スクランブルされた信号情報の読み出しまたは書き込みを行う際のデータの流れを示す図である。

【図3】 コンプライアント記録装置の構成を示す図である。

【図4】 記録装置の記録処理フローを示すフローチャートである。

【図5】 コンプライアント再生装置の構成を示すブロック図である。

【図6】 再生処理フローを示すフローチャートである。

【図7】 パーソナルコンピュータ（PC）記録システムによりコンプライアント記録装置を実現した例を示す図である。

【図8】 PCエンコーダのコントロール部における処理フローを示すフローチャートである。

【図9】 PC記録ドライブのコントロール部における処理フローを示すフローチャートである。

【図10】 パーソナルコンピュータ（PC）再生システムによりコンプライアント再生装置を実現した例を示す図である。

【図11】 PCドライブのコントロール部における処理フローを示すフローチャートである。

【図12】 PCデコーダのコントロール部の処理フローを示すフローチャートである。

【図13】 ディスク種別の情報を転送する際のデータの流れを示す図である。

【図14】 再生システムがDVD-ROMディスクを再生する場合の認証手順とデータ転送手順を示す。

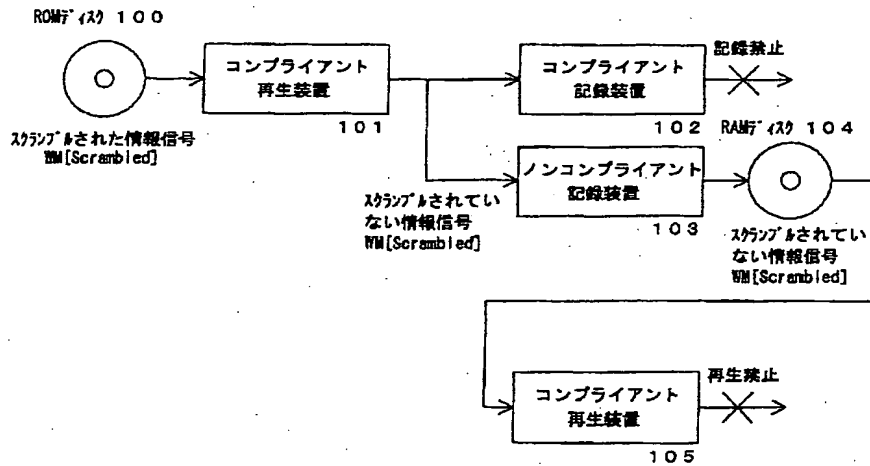
【図15】 再生システムがDVD-Rディスクを再生する場合の認証手順とデータ転送手順を示す。

【図16】 従来の複製制御の原理を示す図である。

#### 【符号の説明】

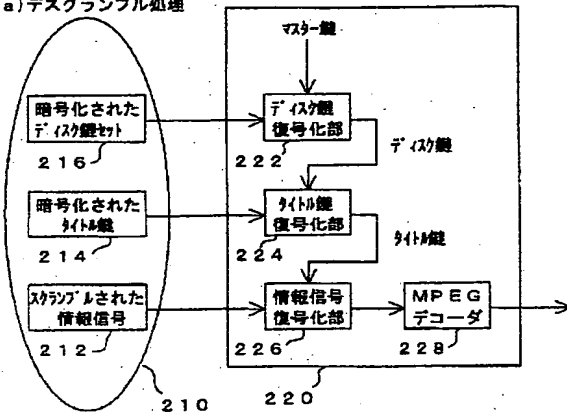
- 101 コンプライアント再生装置
- 102 コンプライアント記録装置
- 105 コンプライアント再生装置
- 301 デジタルI/F
- 302 アナログI/F
- 303 暗号解読部
- 304 エンコード部
- 306 WM書換部
- 307 WMデコード部
- 308 記録制御部
- 309 コントロール部
- 310 スクランブル部
- 311 書込み部
- 313 読み出し部
- 314 ディスク種別判別部
- 401 読み出し部
- 402 デスクランブル部
- 403 スクランブル状態検出部
- 404 ディスク種別判別部
- 405 コントロール部
- 406 WMデコード部
- 407 再生制御部
- 408 デコード部
- 409 アナログI/F
- 410 暗号化部
- 411 デジタルI/F

【図1】

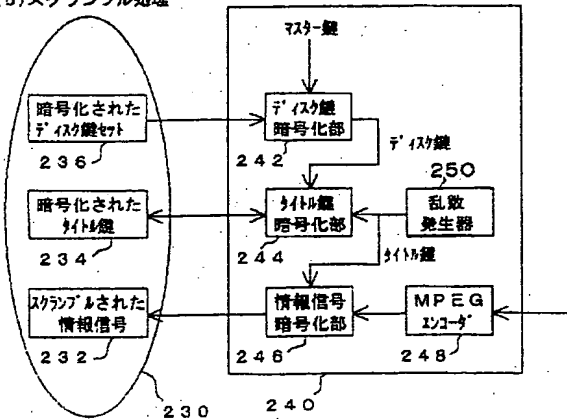


【図2】

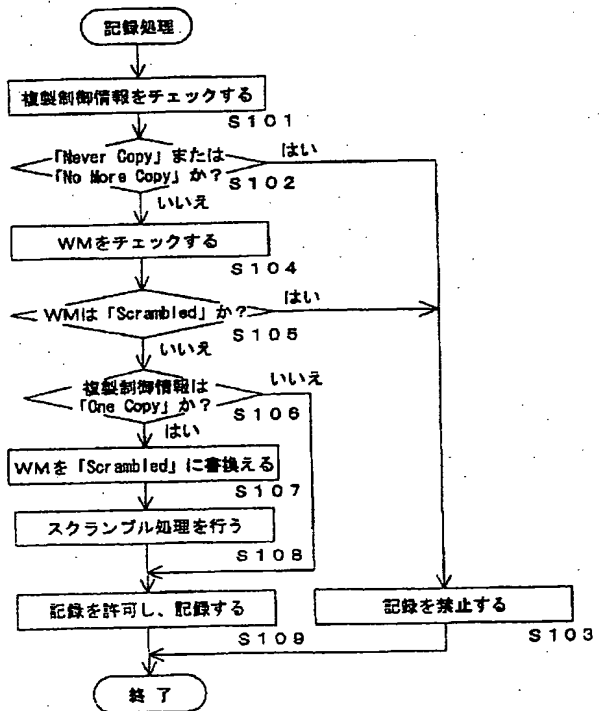
(a) デスクランブル処理



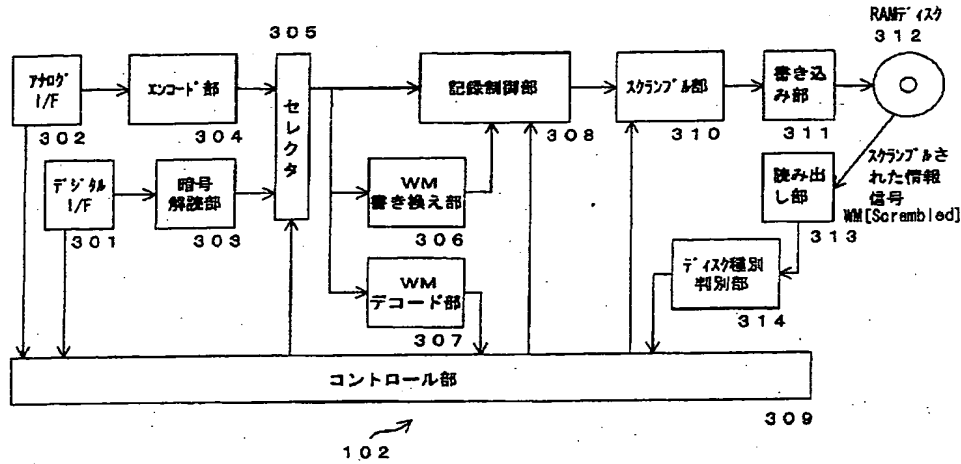
(b) スクランブル処理



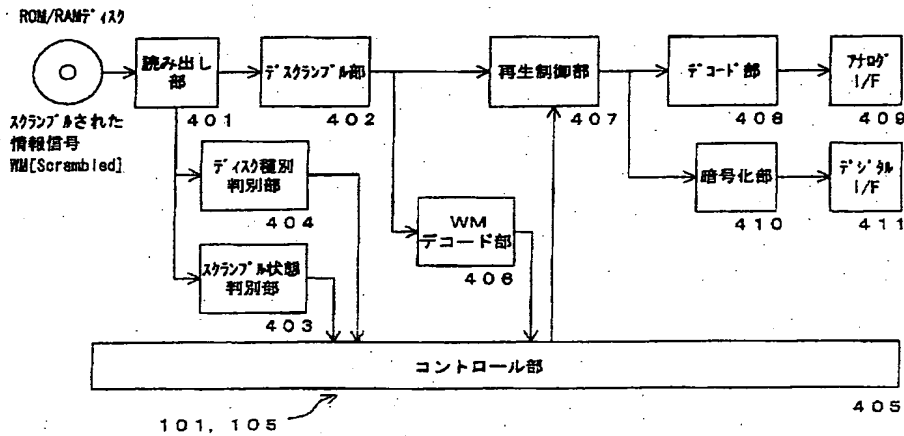
【図4】



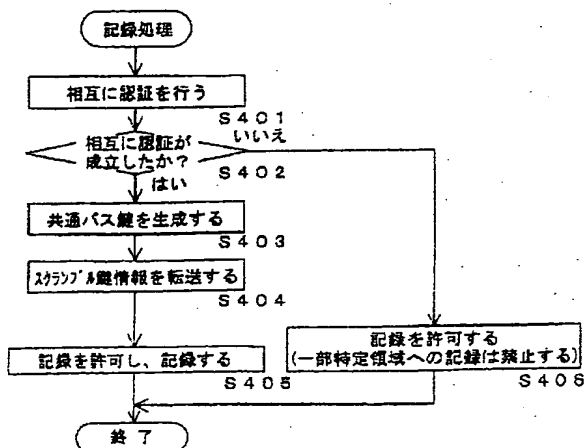
【図3】



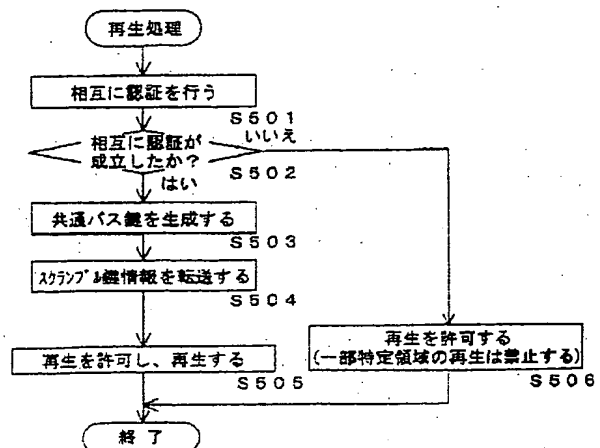
【図5】



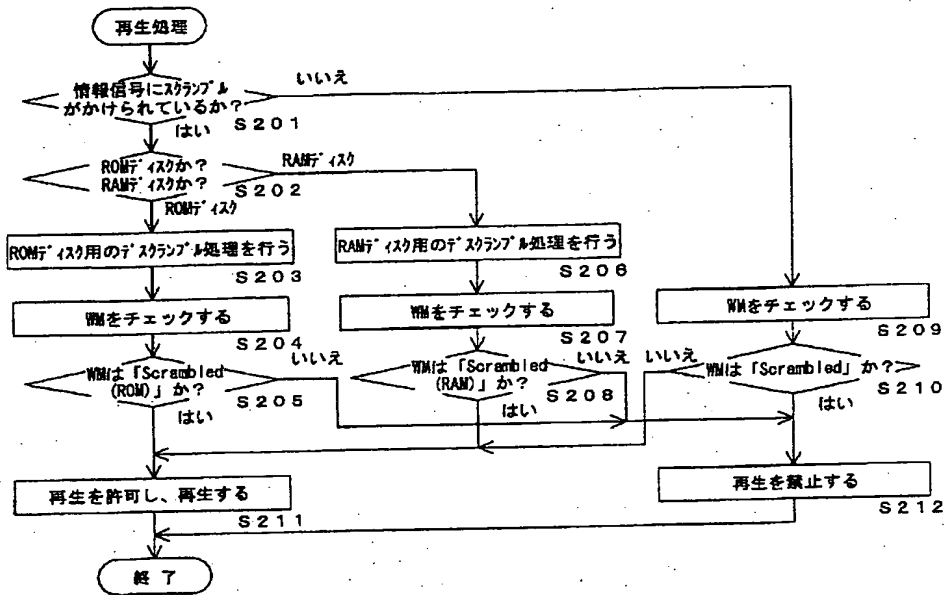
【図9】



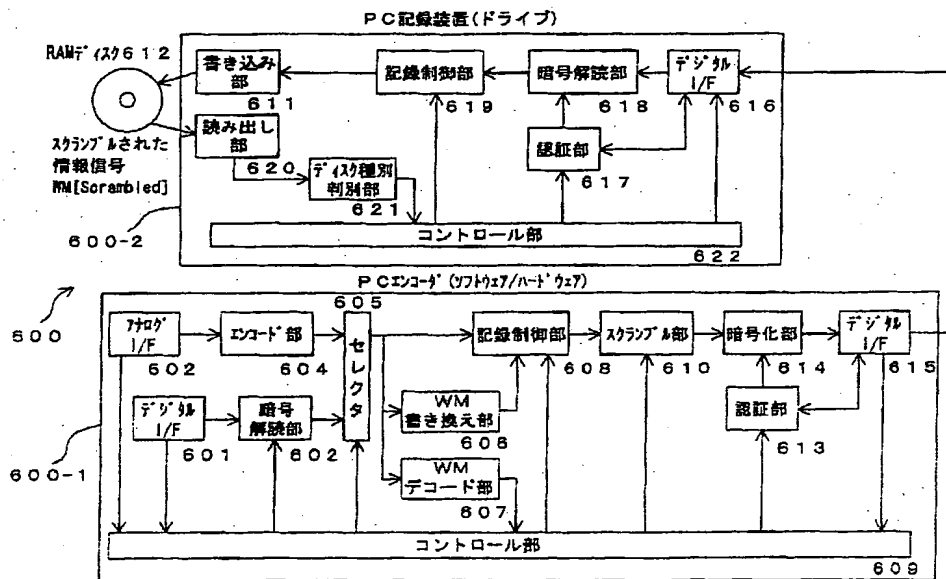
【図11】



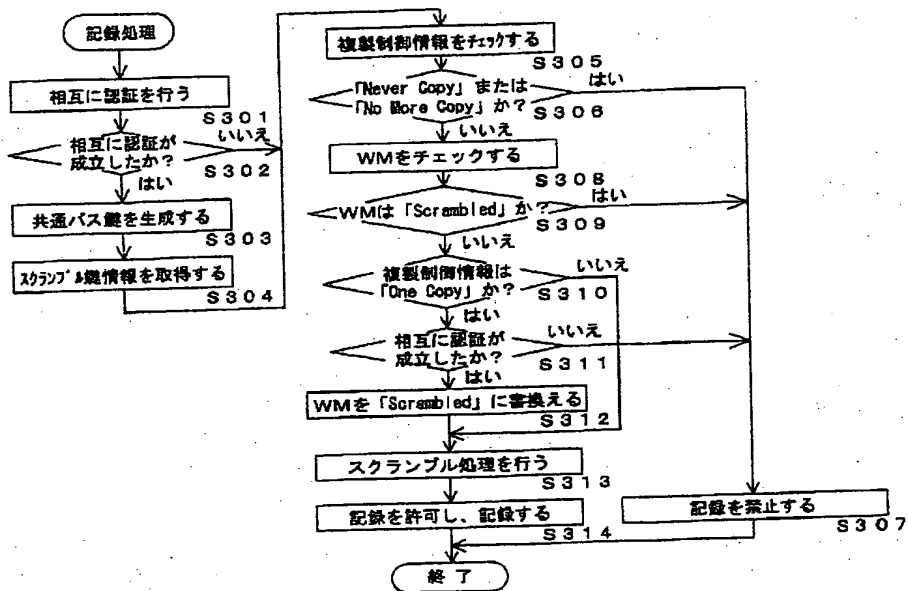
【 6 】



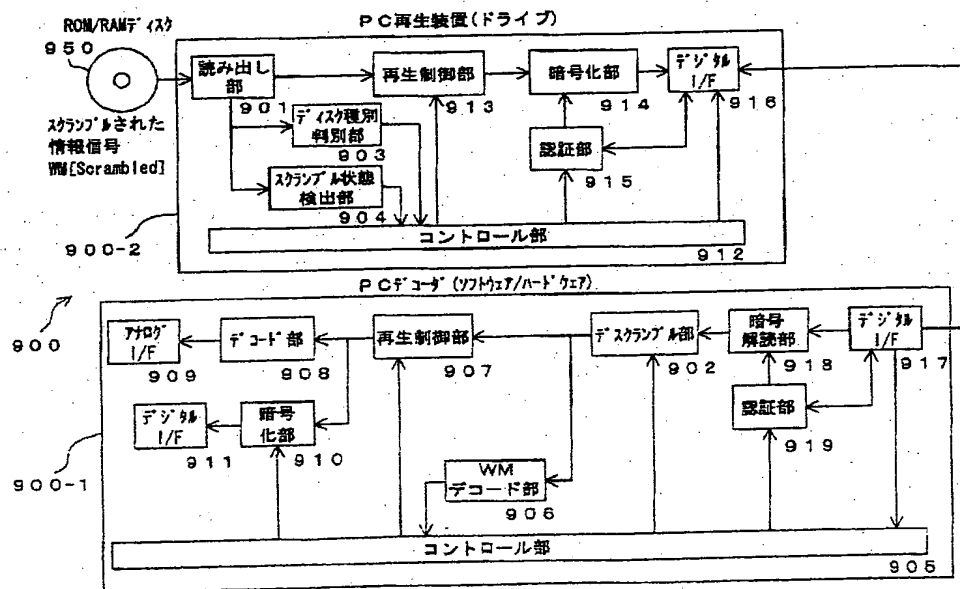
【 7 】

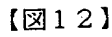


【図8】

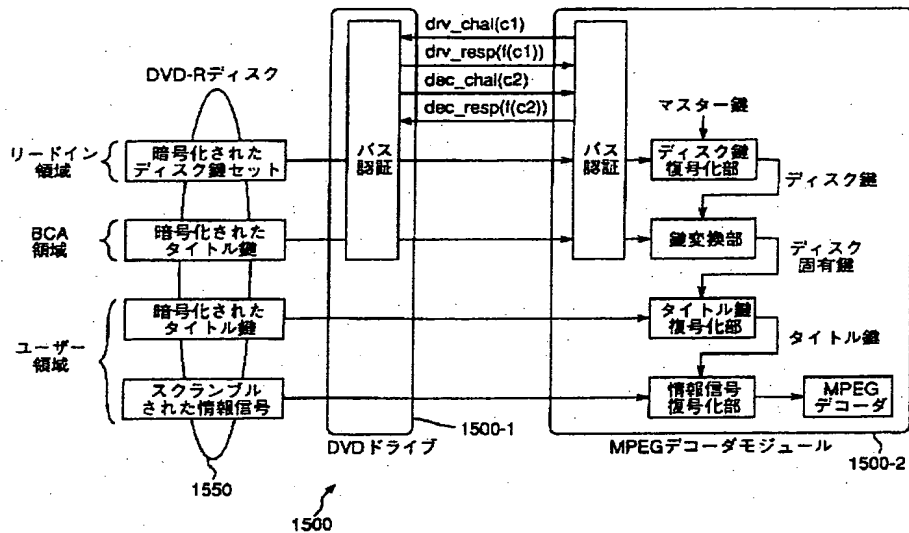


【図10】

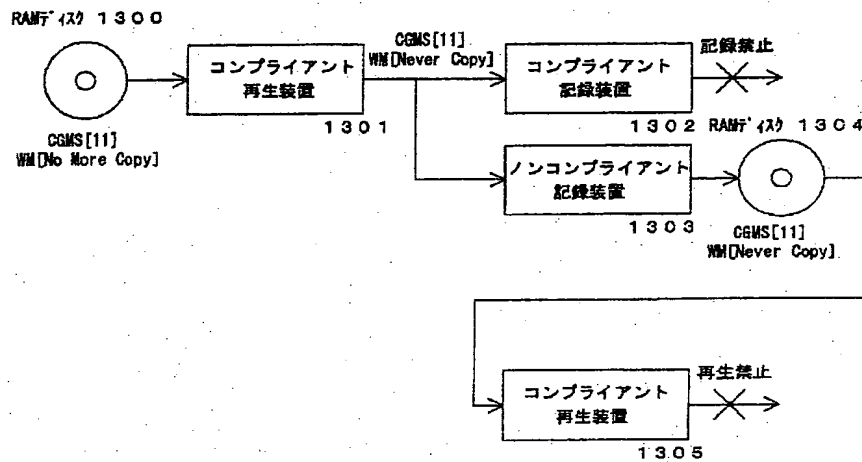




【図15】



【図16】



フロントページの続き

(51)Int. Cl.<sup>7</sup>

識別記号

FI

キーワード(参考)

H04N 1/387  
1/40  
5/91

H04L 9/00  
H04N 1/40  
5/91

601A  
Z  
P

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**